UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,224	07/06/2001	Jeffrey D. Carr	17453US02	4002

23446 7590 05/05/2006

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER
PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/900,224	**Applicant(s)** CARR, JEFFREY D.	
	Examiner Pramila Parthasarathy	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) *1-4,7-9 and 11-18* is/are rejected.

7)□ Claim(s) *5 and 10* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 February 2006* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on April 20, 2006. No new Claims have been added. Claims 1 – 5 and 7 – 18 are pending.

Drawings

2. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because Fig. 6 that was originally filed on 7/6/2001 does not correspond to Fig. 6 that was filed on 2/21/2006. Corrections to Fig. 6 (filed on 2/21/2006) are to be made with respect to new item numbers 70, 200, 202 and 208. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

3. Applicant's arguments see page 7, filed 4/10/2006, with respect to "an appropriate inverse transformation" and the amendments to the claims have been fully considered and are persuasive. The rejection of Claims 1 – 6 and 7 – 18 has been withdrawn.

Response to Remarks/Arguments

4. Applicant's remarks/arguments filed on January 19, 2006, with respect to Claims 1 – 5 and 7 – 18, have been fully considered but they are not persuasive.

Referring to the previous Office action, Examiner had cited relevant portions of the references as a means to illustrate the system as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims.

5. Lotspiech et al. (U.S. Patent Number 6,118,873), teaches a system that includes plural user devices, each of which includes plural device keys selected from a set of device keys. A session number is encrypted with the device key and then transmitted for use in decrypting program. A decryption module that is accessible to each user device can access the device keys of the device and a table (representing the set of device keys such that for each key index variable), each session number that is encrypted only by the device keys in the position. A decryption module is disclosed for receiving at least a session key that represents the index of the local device key.

6. Regarding independent Claim 1, Applicant argues that Lotspiech does not teach "transmitting by the first device the control signal and the encrypted or hashed parameter signal and control signal", "receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal" and "using by the second device the control signal to decrypt or inversely transform the encrypted or hashed parameter signal and control signal". These arguments are not persuasive.

Lotspiech teaches "transmitting by the first device the control signal and the encrypted or hashed parameter signal and control signal" (Column 5 line 55 – Column 6 line 32), wherein a message with session key and encrypted data are transmitted to the receiving device; "receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal" (Column 6 lines 3 – 32), wherein the device receives the session key and encrypted data; and "using by the second device the control signal to decrypt or inversely transform the encrypted or hashed parameter signal and control signal" (Column 6 lines 3 – 46), wherein the device uses the control signal to decrypt the data (program).

7. Regarding independent Claim 7, Applicant argues that Lotspiech does not teach, "receive a control signal comprising an encrypted or hashed form of a parameter signal and a portion of the control signal". This argument is not persuasive. Lotspiech teaches "receive a control signal comprising an encrypted or hashed form of a parameter signal and a portion of the control signal" (Column 6 lines 3 – 32), wherein the device receives the session key and encrypted data.

8. Regarding independent Claim 13, Applicant argues that Lotspiech does not teach, "generating, by the first device, a control signal comprising a key index" and "transmitting, by the first device to the second device, the control signal and the encrypted hash signal". These arguments are not persuasive.

Lotspiech teaches, "generating, by the first device, a control signal comprising a key index" and "transmitting, by the first device to the second device, the control signal and the encrypted hash signal" (Column 5 line 10 – Column 6 line 50), wherein user devices include plural device keys selected from a set of device keys (stored in a table representing the set of device keys such that for each key index variable, each session number that is encrypted only by the device keys in the position), a session number encrypted with the device key and then transmitted for use in decrypting program.

9. Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims 1, 7 and 13. Dependent claims 2 – 5, 8 – 12 and 14 - 18 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending Claims 1 – 5 and 7 – 18 is respectfully maintained.

Allowable Subject Matter

10. Claims 5 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1 – 4, 7 – 9, 11 – 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Lotspiech et al. (U.S. Patent Number 6,118,873).

Regarding claim 1, Lotspiech teaches generating by the first device a control signal and a parameter signal (Summary and Column 5 lines 10 – 20);

encrypting or hashing by the first device a portion of the control signal with the parameter signal to generate an encrypted or hashed parameter signal and control signal (Summary and Column 5 line 55 – Column 6 line 8);

transmitting by the first device to the second device the control signal and the encrypted or hashed parameter signal and control signal (Summary; Column 5 lines 55 – 59 and Column 6 lines 8 – 32);

receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal (Summary and Column 6 lines 3 – 8);

using by the second device the control signal to decrypt or inversely transform the encrypted or hashed parameter signal and control signal (Summary and Column 6 lines 8 – 12); and

generating by the second device a destination parameter signal depending upon a comparison of the control signal and the decrypted or inversely transformed control signal (Summary and Column 6 lines 29 – 50).

Regarding Claim 7, Lotspiech teaches a control logic block to receive a control signal comprising a key index and an encrypted or hashed signal that comprises an encrypted or hashed form of a parameter signal and a portion of the control signal;

an interface operation logic block operably coupled to the control logic block to decrypt or inversely transform the encrypted or hashed signal in accordance with the index to generate a destination parameter signal (Summary and Column 5 line 10 – Column 6 line 50).

Regarding Claim 13, Lotspiech teaches generating by the first device a control signal comprising a key index; using, by the first device, at least a portion of the control signal to obtain a first cryptographic key;

encrypting or hashing using the first cryptographic key, by the first device, a first signal to generate an encrypted or hashed signal; transmitting, by the first device to the second device, the control signal and the encrypted or hashed signal;

receiving by the second device from the first device the control signal and the encrypted or hashed signal; using, by the second device, the key index from the control signal to obtain a second cryptographic key;

decrypting or inversely transforming using the second cryptographic key, by the second device the encrypted or hashed signal to provide a decrypted or inversely transformed signal (Summary and Column 5 line 10 – Column 6 line 50).

As to claim 2, Lotspiech teaches generating by the first device a first key signal using the control signal (Column 5 10 – 29); and

wherein encrypting or hashing comprises using the first key signal (Summary and Column 5 line 55 – Column 6 line 12).

As to claim 3, Lotspiech teaches generating by the second device a second key signal using the control signal (Column 6 lines 29 – 50);

and generating by the second device the destination parameter signal by decrypting or inversely transforming the encrypted parameter or hashed parameter signal using the second key signal (Summary and Column 6 line 29 – Column 6 line 50).

As to claim 4, Lotspiech teaches generating by the first device a key index signal (Column 5 lines 10 – 29);

generating by the first device a key variable signal (Column 5 lines 10 – 29);

transmitting by the first device to the second device the key index signal and the key variable signal (Column 5 lines 55 – Column 6 line 8);

receiving by the second device from the first device the key index signal and the key variable signal (Column 6 lines 3 – 8);

generating by the second device an intermediate key signal using the key index signal and a key table (Column 6 lines 29 – 50);

and generating by the second device the second key signal using the intermediate signal and the variable signal (Column 6 lines 29 – 50).

As to claims 8, 9, 17 and 18, Lotspiech teaches a key table module including indexed cryptographic keys, the key table module operably coupled to the control logic block, the key table module to generate an intermediate key signal using a key index signal received from the control logic block (Column 7 lines 25 – 51);

a key interface stage operably coupled to the key table module and the control logic block for generating a key signal using the intermediate key signal received from the key table module and key variable signal received from the control logic block (Column 7 lines 25 – 51);

and an inverse transformation module operably coupled to the key interface stage and the control logic block, the inverse transformation module to generate the destination parameter signal by decrypting or inversely transforming the encrypted or hashed parameter signal using the key signal received from the key interface stage (Column 6 lines 29 – 50 and Column 7 lines 25 – 51).

As to claim 14, Lotspiech teaches the first signal comprises a parameter signal and a portion of a control signal (Column 5 line 55 – Column 6 line 8);

the decrypted or inversely hashed signal comprises a decrypted or inversely hashed portion of the control signal and a decrypted or inversely transformed parameter signal (Column 6 lies 29 – 50); and

the second device stores the decrypted or inversely hashed parameter signal depending on a comparison of a portion of the control signal received from the first device and the decrypted or inversely transformed portion of the control signal (Column 6 lines 29 – 50 and Column 9 lines 6 – 18).

As to claim 15, Lotspiech teaches the decrypted or inversely transformed portion of the control signal comprises the key index (Column 5 lines 10 – 29).

As to claim 16, Lotspiech teaches transmitting, by the first device to the second device, a destination register signal (Column 5 lines 55 – 59 and Column 6 lines 8 – 32);

receiving, by the second device from the first device, the destination register signal (Column 6 lines 3 – 28);

storing, by the second device, at least a portion the decrypted or inversely transformed signal at a location determined in accordance with the destination register signal (Column 7 lines 4 – 51) .

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CHRISTOPHER REVAK
PRIMARY EXAMINER
CR 4/29/06

Pramila Parthasarathy
April 27, 2006.